UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/432,297	11/02/1999	EARL THOMAS CARTER	2705-76	9858

20575 7590 03/09/2004

MARGER JOHNSON & MCCOLLOM PC
1030 SW MORRISON STREET
PORTLAND, OR 97205

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	PAPER NUMBER
2135	4

DATE MAILED: 03/09/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

1

4

Office Action Summary	**Application No.** 09/432,297	**Applicant(s)** CARTER ET AL.	
	Examiner Thanhnga Truong	**Art Unit** 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *19 December 2003*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gleichauf (US 6, 301, 668 B1), and further in view of Blanchard (US 6, 219, 791 B1).

a. *Referring to claim 1:*

i. Gleichauf teaches:

(1) storing the plurality of encrypted query data packets in a memory **[i.e., data stored in memory or fixed storage on the workstation or other device in which network security system resides (column 5, line 19-21)]** ; and thereafter

(2) scanning the networked computer for a target vulnerability residing therein by sending successive ones of the encrypted-and-stored query data packets to the networked computer and analyzing responses thereto from the networked computer with respect to the characteristic signature **[i.e., Figure 2, scan engine 22 is operable to analyze the network information to identify potential vulnerabilities of internal network 10, and confirm these potential vulnerabilities (column 5, line 63-65). Signature engine 26 is coupled to protocol engine 24 and can perform further analysis tasks in order to detect attacks upon network backbone 14. Signature engine 26 compares monitored traffic with attack signature 30 to comprise a rules-based hierarchy of traffic signatures of known policy violations (column 6, line 37-42)].**

ii. However Gleichauf does not teach:

(1) encrypting a query data packet in accordance with a plurality of encryption keys to produce a plurality of encrypted query data packets, each encrypted query data packet including a defined query field specific to the target vulnerability;

iii. Whereas Blanchard teaches:

(1) Figure 1, encryptor 20, that is for "encrypting a query data packet in accordance with a plurality of encryption keys to produce a plurality of encrypted query data packets, each encrypted query data packet including a defined query field specific to the target vulnerability", includes key generator 24 and exclusive-or (XOR) 22, which receives plain text on signal 15, and receives key 25 from key generator 24. XOR 22 applies key 25 to the plain text to generate encrypted data packets on signal 26 **(column 2, lines 35-39). In addition,**

vi. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such encryptor (such as Figure 2 of Gleichauf) in order to encrypt data packets and compare, and if they do not match, then an error has been detected, and transmission can be stopped **(column 1, line 17-20 of Blanchard).**

v. The ordinary skilled person would have been motivated to:

(1) add such encryptor (such as Figure 2 of Gleichauf) because many communications systems benefit from secure communications provided by encrypted digital data packets **(column 1, line 13-15).**

b. *Referring to claim 2:*

i. Gleichauf further teaches:

(1) in which plural networked computers are so scanned by sending the encrypted-and-stored query data packets to each of plural networked computers and by analyzing responses thereto from each of the plural networked computers **[i.e., Figure 2, scan engine 22 scans devices on internal network, such as workstations 12. It also analyzes the network information to identify potential vulnerabilities of internal network and can direct requests upon the network and**

assess responses to such requests to discover network information (column 5, line 52-65)].

c. *Referring to claim 3:*

i. Gleichauf further teaches:

(1) in which plural ports of plural networked computers are so scanned by sending the encrypted-and-stored query data packets to each of plural ports of each of plural networked computers and by analyzing responses thereto from each of the plural ports of each of the plural networked computers **[i.e., can include port scans (column 4, line 1)].**

d. *Referring to claim 4:*

i. Gleichauf further teaches:

(1) wherein the target vulnerability is Trojan Horse software residing in a port of the networked computer **[i.e., a signature engine is coupled to the network and compares the network data traffic to a plurality of attack signatures to identify attacks upon the network, and each of the attack signatures are designed to detect a particular type of attack upon the network (column 2, line 63-65 and column 8, line 40-42)].**

e. *Referring to claim 5:*

i. This claim has limitations that are similar to those of claim 1, thus it is rejected with the same rationale applied against claim 1 above.

f. *Referring to claim 6:*

i. Blanchard further teaches:

(1) wherein said encrypting is performed for substantially all of the encryption keys within a defined key space **[i.e., Figure 2, trusted key generator 105 provides key 11 to encryptor 21, and provides key 120 o decryptor 31. The use of a trusted key generator is advantageous in part because trusted key generators are commercially available and have undergone independent certification (column 3, line 39-44)].**

g. *Referring to claims 7 and 8:*

i. Gleichauf does not explicitly teaches:

(1) wherein said storing is to a non-volatile memory.

(2) writing the stored plurality of encrypted query data packets from the non-volatile memory to a cache memory prior to said scanning.

ii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) identify those specific kinds of memory (such as Figure 2, storage 36 of Gleichauf) in order to maintain the storing data when the power is lost and since virus checking can be a resource-intensive operation, check files and/or results of checks may be advantageously stored in a cache memory.

iii. The ordinary skilled person would have been motivated to:

(1) clarify these type of memory reside within the storage (such as Figure 2, storage 36 of Gleichauf) because it is a common practice to store data in these type of memory which are well known in the art.

h. *Referring to claim 9:*

i. Gleichauf teaches:

(1) a pre-processor for storing a plurality of such differently encrypted query data packets in a database, the query data packet including one or more fields of data to which a Trojan Horse if resident in a given computer would make a signature response **[i.e., referring to Figure 2, storage 36, that is for "storing a plurality of such differently encrypted query data packets". Scan engine 22 is operable to analyze the network information to identify potential vulnerabilities of internal network 10, and confirm these potential vulnerabilities (column 5, line 63-65). Signature engine 26 is coupled to protocol engine 24 and can perform further analysis tasks in order to detect attacks upon network backbone 14. Signature engine 26 compares monitored traffic with attack signature 30 to comprise a rules-based hierarchy of traffic signatures of known policy violations (column 6, line 37-42)]**;

(2) a memory device for storing the database with the plurality of differently encrypted query data packets **[i.e., Figure 2, storage 36**

comprise memory or fixed storage, that is for "storing the database with the plurality of differently encrypted query data packets" (column 5, line 21-22)];

(3) a transmitter for transmitting said database in a batch to a plurality of computers connected with a network **[i.e., Figure 2, the internal network, indicated generally at 10, can comprise a plurality of workstations 12 coupled to a network backbone 14. Network backbone 14 can comprise, for example, an Ethernet, FDDI, token ring, or other type of network backbone. Protection for internal network 10 can be provided by firewall 16 and a router 18 which are coupled to network backbone 14. Router 18, that is "for transmitting said database in a batch to a plurality of computers connected with a network", serves as a gateway between internal network 10 and an external network 30 (column 4, line 45-53)]**; and

(4) an analyzer for analyzing responses from the plurality of computers to said transmitting, said analyzer recognizing and recording one or more signature responses along with one or more corresponding addresses of the one or more signature-respondent computers **[i.e., Figure 2, scan engine 22 is operable to analyze the network information to identify potential vulnerabilities of internal network 10, and confirm these potential vulnerabilities (column 5, line 63-65). Signature engine 26 is coupled to protocol engine 24 and can perform further analysis tasks in order to detect attacks upon network backbone 14. Signature engine 26 compares monitored traffic with attack signature 30 to comprise a rules-based hierarchy of traffic signatures of known policy violations (column 6, line 37-42)]**.

ii. However Gleichauf does not teach:

(1) a pre-processor for encrypting a query data packet in accordance with a plurality of different keys;

iii. Whereas Blanchard teaches:

(1) Figure 1 shows that a data packet is encrypted by the encryptor 20, which includes a key generator 24, that is for generating "a plurality of different keys". Encrypted data packets leave encryptor 20 on signal 26 and travel to

delay 60 and decryptor 30. Encrypted data is also referred to as "cipher text." **(column 2, line 44-46).** Furthermore, Figure 3 shows a data encryption and verification system in accordance with an alternate embodiment of the present invention. System 300 includes a processor 310, memory 360, that is for "storing a plurality of such differently encrypted query data packets in a database", processor 330, and memory 380. System 300 provides functionality in common with system 10 (Figure 1) **(column 3, lines 45-49).**

vi. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such encryptor/processor (such as Figure 2 of Gleichauf) in order to encrypt data packets and compare, and if they do not match, then an error has been detected, and transmission can be stopped **(column 1, line 17-20 of Blanchard).**

v. The ordinary skilled person would have been motivated to:

(1) add such encryptor/processor (such as Figure 2 of Gleichauf) because many communications systems benefit from secure communications provided by encrypted digital data packets **(column 1, line 13-15).**

i. *Referring to claims 10, 11, 12, 15, 16, and 17:*

i. These claims have limitations that are similar to those of claims 7 and 8, thus it is rejected with the same rationale applied against claims 7 and 8 above.

j. *Referring to claims 13, 18, and 19:*

i. These claims have limitations that are similar to those of claim 6, thus it is rejected with the same rationale applied against claim 6 above.

k. *Referring to claim 14:*

i. Gleichauf teaches:

(1) storing the plurality of encrypted query data packets in a memory **[i.e., data stored in memory or fixed storage on the workstation or other device in which network security system resides (column 5, line 19-21)]** ; and thereafter

(2) scanning the networked computer for a target vulnerability residing therein by transmitting in a batch successive ones of the multiple encrypted-and-stored query data packets to the networked computer and analyzing responses thereto from the networked computer with respect to the characteristic signature [i.e., **Figure 2, scan engine 22 is operable to analyze the network information to identify potential vulnerabilities of internal network 10, and confirm these potential vulnerabilities (column 5, line 63-65). Signature engine 26 is coupled to protocol engine 24 and can perform further analysis tasks in order to detect attacks upon network backbone 14. Signature engine 26 compares monitored traffic with attack signature 30 to comprise a rules-based hierarchy of traffic signatures of known policy violations (column 6, line 37-42). In addition, Router 18, that is "for transmitting said database in a batch to a plurality of computers connected with a network", serves as a gateway between internal network 10 and an external network 30 (column 4, line 52-53)]].**

ii. Although Gleichauf does not teach:

(1) encrypting multiple query data packets in accordance with a plurality of encryption keys to produce a plurality of encrypted query data packets, each encrypted query data packet including a defined query field specific to the target vulnerability;

iii. Whereas Blanchard teaches:

(1) Figure 1, encryptor 20, that is for "encrypting multiple query data packets in accordance with a plurality of encryption keys to produce a plurality of encrypted query data packets, each encrypted query data packet including a defined query field specific to the target vulnerability", includes key generator 24 and exclusive-or (XOR) 22, which receives plain text on signal 15, and receives key 25 from key generator 24. XOR 22 applies key 25 to the plain text to generate encrypted data packets on signal 26 **(column 2, lines 35-39).**

vi. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

(1) include such encryptor (such as Figure 2 of Gleichauf) in order to encrypt data packets and compare, and if they do not match, then an error has been detected, and transmission can be stopped **(column 1, line 17-20 of Blanchard).**

v. The ordinary skilled person would have been motivated to:

(1) add such encryptor (such as Figure 2 of Gleichauf) because many communications systems benefit from secure communications provided by encrypted digital data packets **(column 1, line 13-15).**

Response to Argument

3. Applicant's arguments filed December 19, 2003 have been fully considered but they are not persuasive.

Applicant argues that:

"There is no suggestion in Blanchard of generating one, much less multiple, encrypted query data packets that include query fields specific to a target vulnerability. Claim 1 also specifies storing the plurality of encrypted query data packets in a memory. There is nothing in Blanchard that suggests storing a plurality of the previously encrypted query data packets in memory. Finally, claim 1 specifies scanning the networked computer for a target vulnerability residing therein by sending successive ones of the encrypted-and-stored query data packets to the networked computer and analyzing responses thereto from the networked computer with respect to the characteristic signature. Again there is nothing in Blanchard that remotely suggests sending successive ones of these previously encrypted-and-stored query data packets to networked computers and then analyzing the responses".

Examiner maintains that:

Sufficient reason of combining has been given in the rejection. Gleichauf teaches the claimed subject matter as set forth in the previous rejection to claim 1, and recited in this rejection to claim 1 again, except for the encryption of data packets. However, Blanchard teaches a method and apparatus for encrypting data packets, and for verifying the proper encryption of data packets, without using redundant hardware or software (column 1, lines 37-40). In addition, Blanchard further teaches in Figure 3, processor 310 also generates encrypted packets on signal 320 for transmission outside of system 300. Signal 320 is analogous to signal 68 (Figure 2), in that when no errors are present, signal 320 transmits encrypted and verified data packets outside of system 300 (column 4, lines 12-17). Furthermore, Gleichauf teaches a plurality of analysis tasks are prioritized based upon the network information. The plurality of analysis tasks are to be performed on monitored network data traffic in order to identify attacks upon the network. It is obvious that data packets must containing "a defined query field specific to the target vulnerability" in order to identify attacks upon the network (column 2, lines 51-55).

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 703-305-0327.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-3900.

TBT
March 1, 2004

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100